Office of the Secretary of State
1700 W Washington Phoenix Arizona 85007
(602) 542-0394 Fax (602) 542-1575

April 25, 2002

Linda Skinner, AHCCCS
Guy Wilson, DES

Re Health-e-app electronic signatures

The Policy Authority, in attempting to maintain practices consistent with A.R.S. 41-132, has developed a framework of Electronic Signing Policies for various electronic signing technologies and processes. These Electronic Signing Policies tend to be rather involved documents since they must anticipate the possible range of uses for that technology and related business processes. The Signature Dynamics Electronic Signing Policy describes very generic requirements for the range of possible uses of a variety of biometric signing processes. This memo is to clarify how that document relates to the signing process that AHCCCS and DES contemplate using. This is based on our current understanding of the technology and planned use and should not be considered a complete and final description of what AHCCCS and DES may need to consider or do as they establish this signing process.

As we understand the signing process, the core issues are assuring the signing process complies with statutory requirements that the electronic signature:

1. is unique to the person using it,
2. is under the sole control of that person, and
3. the signature is invalidated if there is any change to the document after the signing.

As this Electronic Signing Policy points out, there is neither a generally accepted technical standard for these biometric based technologies nor a generally accepted method to evaluate the security of the business process employed to use the technology. Therefore, meeting these requirements with this application requires due diligence by AHCCCS and DES that: 1) the technology provides a unique biometric "signature," 2) that another person cannot readily forge it, and 3) that any change in the signed document is detectable. The agencies will need to assure themselves that these requirements are met throughout the "legal" life of the signed electronic document (or that they have a reliable means to copy certify the signed document that will satisfy any legal requirement for retaining the signed document). They will need to re-evaluate these issues whenever the signing tool or signing process changes.

We expect that the agencies and partners have established processes to identify the person signing and that these will readily work for this signing process. We further expect that the technology used will provide sufficient means to verify the unique link between the signer and the signature. The vendor will need to satisfy the agencies that the technology prevents an electronic forgery (change, copy or insertion of the internal representation of the biometric

signature) and that a biometric forgery is at least as detectable as a forgery with pen and paper. (This signing process shouldn't need a Registration Authority as described in the Electronic Signing Policy.)

The agencies and partners will need to give some consideration to what happens if a signature is disputed or an audit requires proof of valid signatures.

The agencies will need to determine the appropriate level of trust this signing process requires. Our expectation is that a Basic level is sufficient but that is a policy decision of the respective agencies (see section 2.4.8.1).

Each Signature Dynamic Tools Provider (or a Signed Electronic Record Management system manager acting as agent for a Signature Dynamic Tools Provider) shall have a mechanism for appropriate Qualified Relying Parties to evaluate and validate a Signature Dynamics electronic signature. This mechanism to evaluate and validate the biometric based unique link between the signer and the signature provide the "shared secret" required within the trust framework described in the Electronic Signing Policy. The minimum functional requirements for this signing process include what is specified in the definitions section of the Policy (5.1).

What we will require is a document (or set of documents) that shows the agreement of the agencies, partners and vendors about:

1. How the Signer is authenticated as the party they represent themselves to be (No formal letter of agreement is needed from a Signer since the described context of their signing should provide evidence of their intent to consider this a "legal" signature.),
2. Who provides the Signature Dynamic signing process tools and agreement that the method used assures the Signer has sole possession of the means of creating their electronic signature,
3. How the electronic signature validity is ascertained by any party with a legal interest,
4. How the record integrity is be ascertained and how that integrity is linked to the Signer's electronic signature with any party with a legal interest able to verify that integrity and link.
5. Agreement that the reception of a record linked to a valid electronic signature and proof of record integrity completes a legally binding signing by the Signer.

We look forward to working with the agencies and their partners on this effort and to seeing it's prompt successful launch.

Russ Savage
Electronic Transactions Liaison
(602) 542-2022
rsavage@sos.state.az.us

cc: Ronald Harris
Michael Totherow